Strengthening Ties Between Process and Security

Carol Woody, CERT, Software Engineering Institute [vita[1]]

2008-08-01 L2 / M[2]

A growing recognition of the importance of security throughout the life cycle has led to new initiatives strengthening ties for security within the SDLC. The role of process in support of security must also be expanded across the full life cycle. Progress has been made in linking security, the SDLC, and process improvement. This article summarizes recent key accomplishments, including an industry-led initiative to harmonize security practices with CMMI, the use of assurance cases, and NIST security considerations in the SDLC.

Introduction

The system development life cycle (SDLC) provides the structure within which technology products are created. This structure embeds organizational policies and practices and regulatory mandates in a repeatable framework that can be tuned to the uniqueness of each project.

A growing recognition of the importance of security considerations throughout the life cycle has led to new initiatives to strengthen the ties for security within the SDLC. The role of process in support of security should not be limited to selected activities at discrete points within the life cycle but must be expanded across the full life cycle to address the following considerations, which were identified at an SEPG 2007 forum [Woody 2007[9]]:

- Security must be a part of the normal organizational information flow and not an add-on when it suits.
- Evidence that an organization is meeting a security standard should be part of the process measurement.
- Security should not just be identified as important; it must be promoted within the organization by management at all levels.
- Process should be viewed as a security enabler—getting the right people at the right place at the right time.
- Security is a separate discipline that must collaborate closely with existing process areas but should not be assumed to fully blend with existing processes.

The SEPG forum also provided observations about the way organizations are considering security within the SDLC [Woody 2007[10]]:

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/887-BSI.html (Woody, Carol)
[3] #dsy1049-BSI_ESA
[4] #dsy1049-BSI_harm
[5] #dsy1049-BSI_conn
[6] #dsy1049-BSI_nist
[7] #dsy1049-BSI_touch
[8] #dsy1049-BSI_SPG
[9] #dsy1049-BSI_woody2007
[10] #dsy1049-BSI_woody2007

- There is awareness of the need to do something but limited understanding of how to go about it effectively.
- Existing standards and regulations are not effectively implemented throughout the life cycle; additional standards and regulations are viewed as unnecessary.
- Unless security capabilities are assessed, the associated security processes and practices will not be improved and will not meet the needs of today’s environment.

A number of initiatives are underway in industry and government to address these perceived process shortcomings. The following have been selected for inclusion in this article:

- Engineering for System Assurance
- Harmonizing Industry Security Practices with the SEI CMMI
- Connecting Security Across the Life Cycle with an Assurance Case
- NIST Security Considerations in the SDLC
- Security Touchpoints in the SDLC
- Security Principles and Guidelines

It is too soon to evaluate the success or limitations of any of these efforts. Many are still under development. This article introduces these efforts and provides sources of further information.

Intended Audience

The target audience for this document includes software development management who recognize the need to strengthen security and assurance within the SDLC. In addition, software engineering process group (SEPG) members who want to enhance the integration of security into their organization’s standard software development processes will find this information of benefit.

Definitions

Assurance case	Provides justification through the use of well articulated arguments, and supporting evidence that specific assurance properties described in the form of claims have been met by a software product, system, or some other grouping of technology components [ISO/IEC CD 15026, 2007, Systems and Software Assurance].
System assurance	Justified confidence that a system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle [NDIA 2007[11]].
Software assurance	The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner [CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006]. Grounds for confidence that an entity meets its relevant needs, goals or objectives for safety, security and dependability, or other characteristics deemed to be critical, and possesses the related

	required properties [ISO/IEC CD 15026:2007, Systems and Software Assurance].

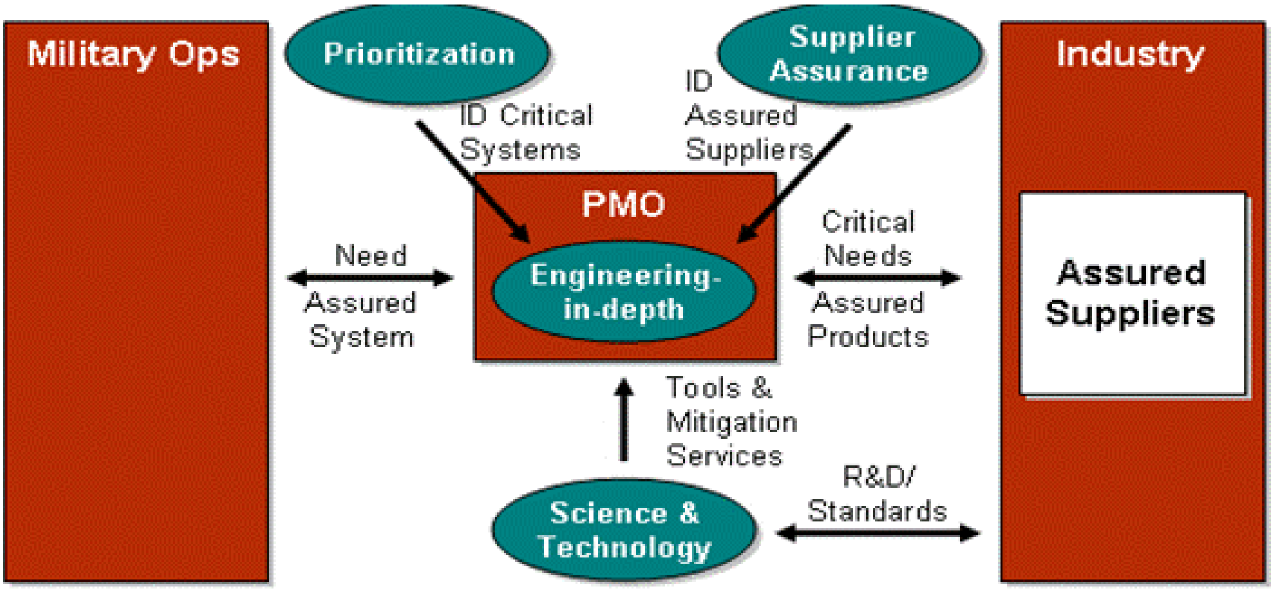
Descriptions of Security Initiatives

Engineering for System Assurance

The National Defense Industrial Association (NDIA) System Assurance Committee has published the "Engineering for System Assurance" guidebook. This document represents a collaboration of government and industry to establish the ways by which organizations can "assure effective functionality of our command, control, communications and related weapon systems with high confidence that the systems are not vulnerable to intrusion and cannot be compromised" [NDIA SA Committee website[12]]. As shown in Figure 1[13] [Komaroff 2006[14]], the Department of Defense (DoD) operational environment connects military operations to technical solutions provided from industry through the program management offices (PMO). The activities performed by the PMO involve prioritization to identify critical systems, engineering-in-depth to establish the acquisition plans and components needed to be built and/or acquired, and supplier assurance to identify appropriately assured suppliers. The PMO draws on science and technology to provide tools and mitigation services and to establish standards for use by selected suppliers.

The guidebook describes the process activities needed to achieve system assurance, a broad umbrella that includes security, safety, reliability, dependability, and other quality attributes. An assurance case is introduced as an appropriate mechanism for assembling and evaluating the assurance attributes of a system.

Figure 1. DoD concept of operations for software assurance



The guidebook is structured using the ISO/IEC 15288 for Systems Life Cycle Processes, but it can be adjusted for any standard SDLC structure. Assurance is recognized as a critical component in each level of processes:

- agreement processes, which consist of acquisition and supply processes
- enterprise processes, which establish the capability to define and manage projects
- project processes, including project planning, project assessment, project control, decision making, risk management, configuration management, and information management

[12] http://www.ndia.org/Template.cfm?Section=Systems_Engineering&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24186

[13] #dsy1049-BSI_figure1

[14] #dsy1049-BSI_komaroff2006

- technical processes, which cover stakeholder requirements definition, requirements analysis, architectural design, implementation, integration, verification, transition, validation, operation, maintenance, and disposal

The activities that provide assurance of the outcome within each SDLC process must be considered and selected for every development effort. Project processes are of particular concern with respect to security. Projects must be planned to have appropriate funding for security, with mechanisms for managing the technical processes to ensure appropriate security. Risk management must consider and mitigate system assurance and security so that project stakeholders do not unknowingly accept risks that have severe financial, legal, and national security implications. A configuration management strategy must include control of configuration items critical to security, including change management for off-the-shelf components to effectively manage security patches and bug fixes. Information management must include protection and marking for proprietary, sensitive, and confidential information.

Technical processes are also extremely critical to system assurance and security. Security requirements are to be tagged with a level of criticality that represents the allowed tolerance for compromise. Functionality must include consideration for both intrinsic (direct delivery of mission functions) and defensive (system security functions) elements. The architectural design must include consideration of least privilege, isolation/containment, monitoring and response for both legitimate and illegitimate actions, tolerance, identification and authentication mechanisms, cryptography, deception, use of interface standards and standard components, and anti-tampering techniques. The design must be evaluated for security weaknesses using appropriate techniques such as threat analysis, failure modes and effects analysis (FMEA), failure modes effects and criticality analysis (FMECA), and fault tree analysis (FTA). Implementation results must be evaluated to ensure, as much as reasonably possible, that known vulnerabilities have not been introduced.

Specific guidance for DoD projects that links assurance deliverables with appropriate phases of the DoD Life Cycle Framework is provided. Mappings of guidebook content to standards such as ISO/IEC 15288, relevant sections of DoD Instruction 5000.2, relevant DoD information assurance (IA) controls documented in DoD Instruction 8500.2, and the Defense Acquisition Guide (DAG) are included.

The guidebook [NDIA 2008[15]] is available for download and comment (http://www.acq.osd.mil/sse/ssa/initiat_sa.html).

Harmonizing Industry Security Practices with the SEI CMMI

A working group of industry representatives led by participants from Booz Allen Hamilton, Lockheed-Martin, and Motorola formed in 2007 as a result of discussions at the Security Birds of a Feather (BOF) at SEPG 2007. Their primary drive stemmed from the inconsistent treatment of safety and security concerns in CMMI®-DEV. In addition, they identified insufficient assurance detail in required and expected components and lack of traceability to assurance source standards for compliance validation. The goal of the working group is a harmonization of existing security standards with CMMI so that an increased focus on security and assurance will be easy for CMMI users to implement.

The following standards and related assurance projects addressing security, safety, and dependability have been considered as the landscape of assurance for support in the harmonization work as well as industry best practices in use at one or more of the working group membership organizations:

- ISO/IEC SC22 – OWG: Vulnerabilities (OWGV) – Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use
- ISO/IEC 15408 Common Criteria for IT Security Evaluation
- ISO/IEC 15443 Framework for IT Security Assurance (3 parts)
- ISO/IEC 21827 System and Security Engineering Capability Maturity Model (SSE CMM) revision
- ISO/IEC 2700 series – Information Security Management System (ISMS)

[15] #dsy1049-BSI_ndia2008

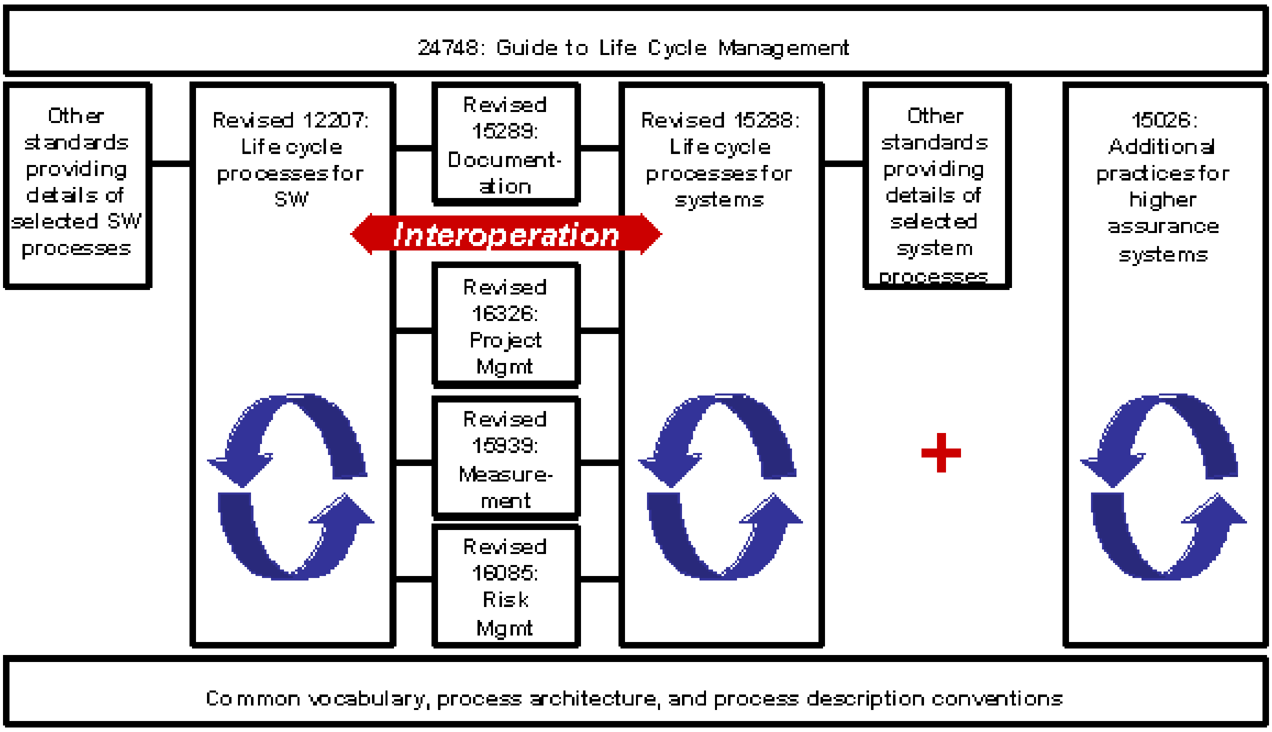
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (7 parts)
- IEC 6-300 Series, Dependability Management
- IEC 61713 Software dependability through the software life-cycle processes – Application guide
- IEC 60812 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FEMA)
- IEC 61025 Fault Tree Analysis (FTA)

Additionally, the following standards for embedding assurance process details into life cycle processes were considered:

- ISO 24748: Guide to Life Cycle Management
- ISO 12207 (revised): Life Cycle Processes for Software
- ISO 15289 (revised): Documentation
- ISO 16326 (revised): Project Management
- ISO 15939 (revised): Measurement
- ISO 16085 (revised): Risk Management
- ISO 15288 (revised): Life Cycle Processes for Systems
- ISO 15026: Assurance Case

The relationships among these life cycle process standards are shown in Figure 2[17].

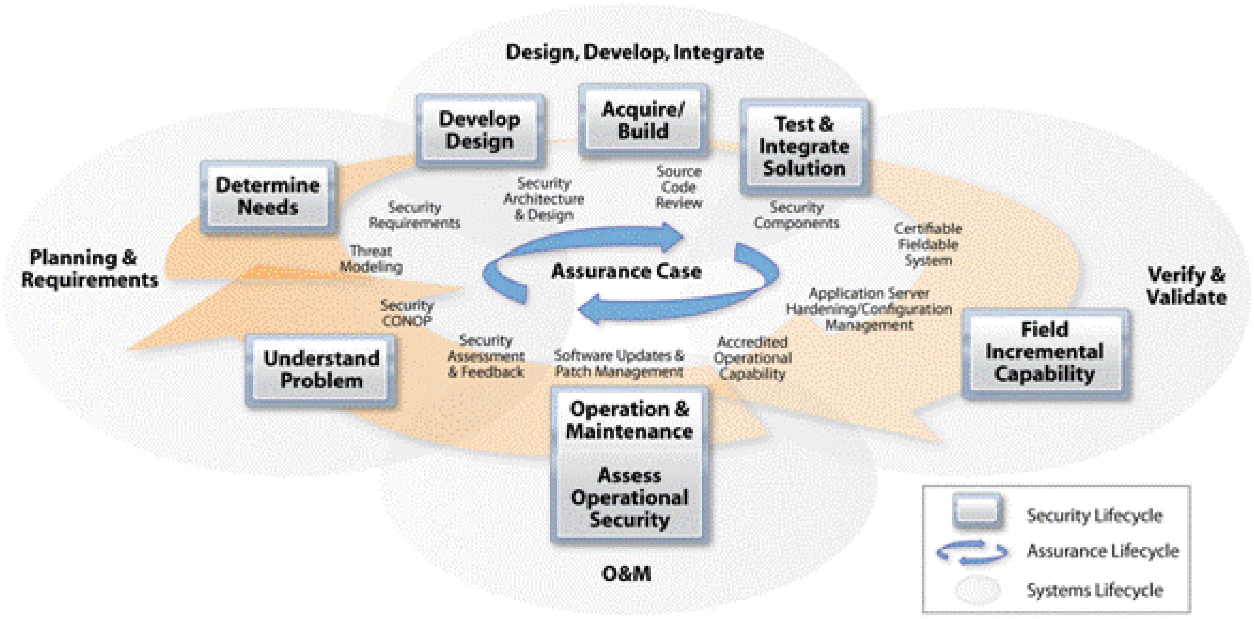
Figure 2. Assurance standards connect to life cycle standards [Moore 2007[18]]


24748: Guide to Life Cycle Management
Other standards providing details of selected SW processes
Revised 12207: Life cycle processes for SW
Revised 15289: Document-ation
Interoperation
Revised 16326: Project Mgmt
Revised 15939: Measure-ment
Revised 16085: Risk Mgmt
Revised 15288: Life cycle processes for systems
Other standards providing details of selected system processes
+
15026: Additional practices for higher assurance systems
Common vocabulary, process architecture, and process description conventions

Security and assurance life cycles are anticipated to flow in conjunction with the system and software life cycle, providing a means for harmonizing the work of IT with security and assurance. The blending of these three life cycles is shown in Figure 3[19].

[17] #dsy1049-BSI_figure2
[18] #dsy1049-BSI_moore2007
[19] #dsy1049-BSI_figure3

Figure 3. System, assurance, and security life cycles are interrelated [Croll 2008[20]]


Design, Develop, Integrate
Develop Design
Acquire/ Build
Test & Integrate Solution
Determine Needs
Security Requirements
Security Architecture & Design
Source Code Review
Security Components
Planning & Requirements
Threat Modeling
Assurance Case
Certifiable Fieldable System
Verify & Validate
Security CONOP
Application Server Hardening/Configuration Management
Understand Problem
Security Assessment & Feedback
Software Updates & Patch Management
Accredited Operational Capability
Field Incremental Capability
Operation & Maintenance
Assess Operational Security
O&M
Security Lifecycle
Assurance Lifecycle
Systems Lifecycle

The efforts of the working group are still underway. Portions of the working group material have been presented at two conferences: SEPG 2008 [Beard 2008[21]] and Systems and Software Technology Conference (SSTC) 2008 [Croll 2008[22]]. Collaboration with other industry and government efforts continues to provide an avenue to build on the knowledge of the security and assurance community and stay current with parallel research efforts. Table 1 includes draft goals, practices, and subpractices for assurance process management, assurance project management, assurance engineering, and assurance support activities cross referenced to the target CMMI process area and target CMMI goal.

Table 1. Process Reference Model for Assurance Mapped to Proposed CMMI PA[23] [PDF download]

This model can be used on its own or in conjunction with other standards and frameworks such as the SEI CMMI and ISO-9000.

The working group welcomes questions and feedback as they continue to develop the harmonization. The harmonization working group can be contacted through the DHS Processes and Practices Working Group co-chairs at swawg-process@cert.org[24].

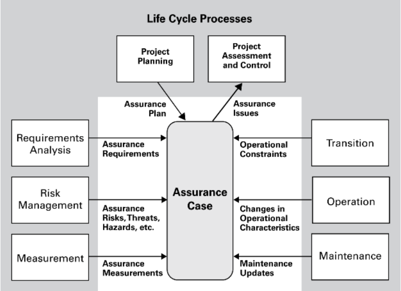
Connecting Security Across the Life Cycle with an Assurance Case

The software assurance case has been proposed within ISO 15026 as the central artifact that establishes with confidence the achievement of security, safety, and reliability by a software or system product. The life cycle processes for planning, monitoring, achieving, and demonstrating for decision-making contribute to the development and refinement of the assurance case. A close linking of the assurance case to relevant life cycle processes as shown in Figure 4[25] provides for the use of the assurance case as the vehicle for informing stakeholders of the progress toward achievement of assurance and allows it to become the operational perspective of assurance achievement. Within the activities of Project Planning must be the development of an assurance plan. Through Project Assessment and Control, assurance issues are identified and evaluated. Requirements Analysis includes activities to identify and prioritize assurance requirements. Risk

[20] #dsy1049-BSI_croll2008
[21] #dsy1049-BSI_beard2008
[22] #dsy1049-BSI_croll2008
[23] http://buildsecurityin.us-cert.gov/bsi/1043-BSI.html (Process Reference Model)
[24] mailto:swawg-process@cert.org
[25] #dsy1049-BSI_figure4

Management activities identify the risks, threats, and hazards that drive the assurance case. Measurement processes must include assurance measurements. The assurance case provides operational constraints to Transition processes. Also, over the operational life of the software or system, an interface with Operation would identify changes in operational characteristics that may trigger the need for adjusting the assurance case. Through a Maintenance interface, assurance related information about maintenance updates should be provided.

Figure 4. Some relationships of the assurance case to life cycle processes [ISO/IEC CD 15026]



In recognition that business work processes increasingly require integration across multiple systems to support, for example a just-in-time supply chain for manufacturing, the assurance case can be positioned as the connecting artifact that brings information about the confidence of required qualities from software and system components into the business process. In addition, software and systems may be used in the future in ways not originally part of the designed capabilities. An assurance case for each of the systems and software components can inform the business process of the level of available assurance and strengthen operational risk management decisions. Likewise a separate assurance case could be constructed from the business process and inform the assurance requirements for systems and software components planned for use within the business process. An example of a way in which a business process could be used to construct an assurance case to inform the development of systems and software is described for survivability in *Survivability Assurance for System of Systems* [Ellison 2008[26]].

NIST Security Considerations in the SDLC

Publication SP 800-64 revision 2 (DRAFT) [Kissel 2008[27]] articulates the steps needed to integrate a minimum set of critical security milestones into the SDLC for all United States federal agencies. These activities supplement the risk management framework described in NIST SP 800-39. For effective consideration of security in a project, the organization must incorporate security risk considerations into the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes. This organizational level informs the development project in the critical areas of planning, acquisition, project monitoring, and deployment. By specifically addressing risk management into milestones, deliverables, control gates, and interdependencies, measurement and enforcement of security requirements can be addressed across the life cycle.

In the project initiation phase, the following security considerations are needed:

- Determine business requirements in terms of confidentiality, integrity, and availability.
- Determine information categorization and special handling requirements for personally identifiable information as it is created, stored, and transmitted.
- Determine privacy requirements.

In the project development phase, the following are needed for effective security consideration:

- Supplement the risk assessment to include a security risk assessment.
- Analyze security controls and design security architecture.
- Perform functional and security testing.

[26] #dsy1049-BSI_ellison2008
[27] #dsy1049-BSI_kissel2008

- Develop, plan, and initiate documents for certification and accreditation.

For the implementation phase of a project, the following security considerations are needed:

- Integrate the system being developed into the operational environment.
- Validate security controls.
- Conduct system certification and accreditation activities.

During system operations and maintenance, security must be considered in the following areas:

- conducting operational readiness reviews
- managing configuration of the system
- monitoring of security controls
- reauthorization when required

System disposal also has critical security implications as follows:

- developing and executing a transition plan for removal
- ensuring information preservation
- sanitizing media
- disposal of hardware and software
- system shut-down

Security Touchpoints in the SDLC

Security touchpoints have been identified as a lightweight strategy for initiating improved security. By embedding key activities into the SDLC processes that address the quality of the developed code and including some specific considerations for security at critical points in development, improvement in security can be achieved [McGraw 2006[28]].

Start with code reviews and architectural risk analysis. The first will identify common mistakes in the code that may not be seen by the developing programmer. Static analysis tools can help in identifying common vulnerabilities early in development for easier correction. The second, architectural risk analysis, provides a means of identifying design flaws such as poor compartmentalization and improper authentication of services.

Next, add penetration testing to identify ways in which the software interacts insecurely with its real environment. Risk-based security tests should be added to ensure the security functionality is working properly and common attack patterns are properly handled. In addition, look at the requirements development to incorporate abuse cases that establish how the system should behave when something that should not happen does occur. Also make security requirements explicit in describing how the system should function to provide effective confidentiality, integrity, and availability. Security operations are also needed to support the need to recognize, resist, and recover from an attack on a vulnerability that was missed in design and development.

By using external resources instead of those actively engaged within development, “fresh eyes” have a better chance of spotting problems than those that have already been looking at the components of the system extensively.

Security Principles and Guidelines

The Institute for Infrastructure and Information Assurance has published *Toward an Organization for Software System Security Principles and Guidelines* [Redwine 2008[29]] to provide a basis for teaching and learning about security. Though intended for an academic audience, this material is well positioned to provide conceptual mastery to a broader audience. The SDLC is projected as a stream (referred to as the

[28] #dsy1049-BSI_mcgraw2006

[29] #dsy1049-BSI_redwine2008

system) that moves in parallel to the adverse and the environment streams. The adverse stream includes “malicious and non-malicious attempts to violate security or exploit violations.” The environment stream incorporates “aspects of the environments with implications for security-related interactions across the software system’s lifespan and possibly beyond” [Redwine 2008[30]].

With increased understanding of the interrelationships among these three streams, an organization can better evaluate their existing SDLC procedures and practices to identify the critical points where security must be considered.

References

[Beard 2008]
Beard, Dennis, Moss, Michele, & Nadworny, Margaret. “Process Reference Model for Assurance.” *SEPG 2008* (CD-ROM). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2008.

[Croll 2008]
Croll, Paul & Moss, Michele. “Leveraging Models and Standards for Assurance.” SSTC Las Vegas, April 30, 2008.

[Ellison 2008]
Ellison, R., Goodenough, J., Weinstock, C., & Woody, C. *Survivability Assurance for System of Systems* (CMU/SEI-2008-TR-008). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2008.

[Kissel 2008]
Kissel, Richard, Stine, Kevin, Scholl, Matthew, Rossman, Hart, Fahlsing, Jim, & Gulick, Jessica. *Security Considerations in the System Development Lifecycle*, Revision 2 (DRAFT) (NIST Special Publication 800-64). National Institute of Standards and Technology, March 2008.

[Komaroff 2006]

Komaroff, Mitchell. "DoD Software Assurance Concept of Operations[31]," June 27, 2006.

[McGraw 2006]
McGraw, Gary. *Software Security: Building Security In*. Boston, MA: Addison-Wesley Professional, 2006 (ISBN 0-321-35670-5).

[Moore 2007]
Moore, J. “SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee.” Executive Committee Winter Plenary Meeting, February 2007.

[NDIA 2008]
National Defense Industrial Association (NDIA) System Assurance Committee. *Engineering for System Assurance* (draft). Arlington, VA: NDIA, 2008.

[Redwine 2008]

Redwine, Samuel T. Jr. *Towards an Organization for Software System Security Principles and Guidelines*[32], version 1.0 (IIIA Technical Paper 08-01). Institute for Infrastructure and Information Assurance, James Madison University, February 2008.

[Woody 2007]

Woody, Carol. *Process Improvement Should Link to Security: SEPG 2007 Security Track Recap*[33] (CMU/SEI-2007-TN-025). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007.

[30] #dsy1049-BSI_redwine2008

[31] http://www.afei.org/brochure/6a08/documents/Komaroff_CONOPS27June06.pdf

[32] http://www.jmu.edu/iiia/webdocs/Reports/SwA_Principles_Organization-sm.pdf

[33] http://www.sei.cmu.edu/pub/documents/07.reports/07tn025.pdf

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[1] mailto:permission@sei.cmu.edu